Lista delle domande di teoria possibili

1) Il salt è una variazione random inserita dal sistema all'atto della memorizzazione della password scelta → VERO *(FREQ. - 3)*

---

2) I sistemi a sfida e risposta sono tipicamente implementati condividendo un *segreto* come ad esempio una chiave simmetrica. → FALSO *(FREQ. 3)*

Un esempio di challenge & response sono i sistemi a chiave asimmetrica, dove la challenge è la public key e la response è la private key.

---

3) In Unix il comando passwd si usa per verificare la robustezza della password. → FALSO *(FREQ. - 2)*

`passwd` è il comando che ci permette di cambiare la password.

---

4) Tra i fattori di autenticazione c'è qualcosa che si conosce (Password, PIN) → VERO

---

5) FIDO alliance è un sistema di generazione degli OTP → FALSO *(FREQ. 2)*

La FIDO alliance è gruppo di aziende leader come Google e Microsoft che sviluppano standard per consentire un'esperienza di autenticazione più semplice e sicura su siti web e servizi mobile, creando ad esempio U2F e UAF.

---

6) Il controllo dell'accesso è decidere se un soggetto può eseguire una specifica operazione su di un oggetto → VERO (pretty self explanatory)

---

7) Il comando find / -type f -perm /6000 permette di trovare i file coi bit SUID e SGID impostati a 1. → FALSO.

In realtà penso che il prof si sia sbagliato, siccome il comando fa esattamente quello. Questa domanda però ad ogni prova ha una risposta corretta diversa...

---

8) Il SUID è il bit che permette di lanciare con sudo il programma su cui è settato → FALSO *(FREQ. 3)*

Il SUID è il bit che esegue il programma come se fosse l'owner del file.

---

9) I due paradigmi fondamentali per il controllo dell'accesso sono DAC (Discretionary access control) e TAC (Tertiary access control) → FALSO

I due paradigmi fondamentali sono:

- **DAC (Discretionary access control)**:
  - Ogni oggetto ha un proprietario
  - Il proprietario decide i permessi
- **MAC (Mandatory access control)**:
  - La proprietà di un oggetto non consente di modificarne i permessi
  - C'è una policy centralizzata decisa da un security manager

---

10) Le capability list sono delle liste associate a ogni *soggetto* del sistema → VERO *(FREQ. 2)*

---

11) Nei cifrari a trasposizione le statistiche dei digrammi e trigrammi permettono di dedurre la dimensione della tabella di cifratura → VERO *(FREQ. 3)*

---

12) La proprietà di diffusione misura il grado in cui le proprietà statistiche degli elementi del testo cifrato vengono sparse sugli elementi del testo in chiaro → FALSO

Notare bene il testo:
"*La proprietà di diffusione misura il grado in cui le proprietà statistiche degli elementi del testo cifrato vengono sparse sugli elementi del testo in chiaro*"
Ovviamente, il testo cifrato non influenza in alcun modo il testo in chiaro. La frase vera sarebbe:
"*La proprietà di diffusione misura il grado in cui le proprietà statistiche degli elementi del* ***testo in chiaro*** *vengono sparse sugli elementi del* ***testo cifrato***"

---

13) Nell'attacco dei cifrari a sostiuzioni il fatto che alcune lettere siano più frequenti di altri nel linguaggio naturale non ha nessuna importanza → FALSO

Il fatto che alcune lettere siano più frequenti di altre facilita molto il cracking di questi cifrari.

---

14) Nel cifrario con sostituzione monoalfabetica sull'alfabeto inglese lo spazio delle chiavi è grande 26! - VERO *(freq. 2)*

---

15) Nel test di Kasiski si impiega la fattorizzazione delle distanze e la scelta di quelle con un fattore comune – VERO *(FREQ. 3)*

---

16) Il miglior attacco a RSA è la ricerca dei fattori del modulo – VERO *(FREQ. 3)*

---

17) DH e RSA hanno scopi differenti: quello di DH è scambiare una chiave condivisa tra due parti – VERO

N.B.: non sono schemi diversi, ma hanno ognuno un suo scopo.

---

18) Diffie-Hellmann è uno schema di cifratura a chiave simmetrica – FALSO

Diffie-Hellmann rappresenta uno "strategia" di scambio di un segreto.

---

19) DH e RSA hanno scopi differenti: quello di RSA é di essere molto più veloce nella fase di cifratura/decifrazione – FALSO *(FREQ. 3)*

Prima di tutto, come abbiamo detto prima, è come confrontare mele e pere.
Secondo, RSA è molto più lento della cifratura a chiave pubblica, alla quale la domanda sta cercando di ingannare il lettore.

---

20) CBC sta per Cipher Block Chaining e consiste nel Cifrare un blocco modificandolo col

contributo del blocco cifrato precedente – VERO *(freq. 2)*

---

21) Le chiavi di autenticazione usate da Secure Boot sono aggiornabili senza interruzioni di servizio – FALSO *(FREQ. 4)*

È falso siccome quando sono da aggiornare, l'immagine stessa del BIOS UEFI deve essere firmata con le chiavi private del fornitore, rendendo poi disponibile la propria chiave pubblica iscrivendola nel firmware. Questo passaggio richiede un reboot.

---

22) È possibile danneggiare fisicamente un sistema attraverso una porta USB – VERO *(FREQ. 2)*

---

23) La collocazione di sistemi in cloud migliora (generalmente) la disponibilità dei servizi – VERO *(FREQ. 3)*

---

24) La cifratura dei dischi protegge da qualsiasi tentativo di esfiltrazione dei dati – FALSO *(FREQ. 4)*

Se uno prende il disco, può comunque prendere dei dati utili o facendo bruteforcing, e ha tutto il tempo che vuole.

---

25) L'approccio default deny su firewall significa che tutto il traffico viene bloccato – FALSO *(freq. 2)*

Domanda traboccheto. Vuol dire semplicemente che di default, se non è specificata una regola, il pacchetto viene bloccato. Altrimenti, se la regola viene matchata, il pacchetto viene spedito.

---

26) Un Intrusion Detection System può bloccare un attacco in corso – FALSO *(FREQ. 2)*

Un IDS, di base, non può bloccare un attacco in corso. In caso contrario, si parla di IPS (Intrusion Prevention System).

---

27) Un vantaggio degli Host-based IDS è che possono classificare più accuratamente il rischio associato a un pacchetto di rete – VERO *(FREQ. 3)*

---

28) Il tasso di "falsi positivi" non è un parametro importante per la qualità di un IDS – FALSO *(FREQ. 3)*

Ovviamente è importante: se abbiamo troppi falsi positivi, ci sono troppi controlli manuali e l'utente tenderà a non usare/ignorare l'IDS.

---

29) Un vantaggio dei Network-based IDS è che non interferiscono col funzionamento dei sistemi monitorati – VERO

---

30) Suricata può funzionare sia da IDS che da IPS – VERO *(freq. 2)*

---

31) HTTPS è HTTP su di un canale di comunicazione cifrato - VERO

---

32) L'IP spoofing consiste nel cercare di scoprire l'IP di una macchina vittima – FALSO

Consiste nel far credere che il proprio IP sia un altro, diverso da quello effettivo.

---

33) Lo sniffing può compromettere la riservatezza dei dati – VERO *(FREQ. 2)*

---

34) Gli attacchi passivi non modificano i dati in transito – VERO *(FREQ. 4)*

---

35) Lo sniffing NON richiede accesso fisico alla rete – FALSO *(freq. 2)*

Trabocchetto.
Devi essere collegato alla rete direttamente alla rete su cui viaggiano i pacchetti. Se viaggiano in modo wireless, devi essere nei pressi dello scambio per poter rilevare e sniffare.

---

36) I canarini sono un meccanismo di protezione del kernel linux per segnalare un overflow in memoria. - FALSO *(FREQ. 4)*

Non sono inseriti dal kernel linux, ma dal compilatore di tali programmi.

---

37) ASLR è un meccanismo di protezione del kernel linux per randomizzare gli spazi di memoria – VERO *(freq. 2)*

---

38) Il comando con codice esadecimale 0x90 dell'assembler x86 è del tutto inutile ai fini della realizzazione di payload – FALSO

Voglio dire, lo usiamo sempre in bof, specialmente quando dobbiamo fare esecuzioni di funzioni interne o altro, e abbiamo lo stack eseguibile.

---

39) Inserire un ritardo di pochi secondi tra due login errate non è una misura efficace per mitigare gli attacchi brute force – FALSO

Può fare una grande differenza, per questo che è molto usato.

---

40) La strcpy in linguaggio C non è una funzione a rischio di generare vulnerabilità di buffer overflow – FALSO *(FREQ. 3)*

È una delle funzioni vulnerabili.

---

41) Nell'autenticazione attiva Prover e Verifier si scambiano ogni volta un dato diverso – VERO ***(freq. 2)***

---

42) Lo scopo del TOTP è quello di forzare l'utente a cambiare periodicamente la password - FALSO

Con TOTP si intende la **timed one-time password**, che è una password aggiuntiva, sottoforma di token è valida solo per un utilizzo ed è limitata nel tempo.

43) Le ACL sono liste associate ad ogni soggetto del sistema – FALSO *(FREQ. 3)*

Le ACL sono associate ad ogni risorsa, mentre le capability list sono associate ad ogni soggetto.

---

44) Le ACL e le Capabilities sono la stessa cosa – FALSO *(freq. 2)*

Ovviamente non lo sono.

---

45) I bit di autorizzazione standard nel filesystem Unix sono di 3 tipi R,W,X (read,write,execute) – VERO *(FREQ. 2)*

---

46) Ogni permesso su di un file in NTFS può assumere due soli valori (concesso o negato) – FALSO *(freq. 2)*

Ogni permesso, in NTFS può essere allow, deny o non impostato.

---

47) Nei cifrari a sostituzione polialfabetica conoscere il contenuto di una parte del messaggio non aiuta la decifrazione dell'intero testo – FALSO *(FREQ. 3)*

Aiuta comunque, siccome possiamo notare il ripetere periodico delle sostituzioni.

---

48) L'Indice di Coincidenza è la probabilità che due lettere scelte a caso in un testo siano *diverse* – FALSO *(FREQ. 2)*

Trabocchetto.
L'Indice di Coincidenza è la probabilità che due lettere scelte a caso in un testo siano *uguali.*

---

49) Nei cifrari a sostituzione polialfabetica le frequenze di un carattere cifrato derivano da contributi di diversi caratteri in chiaro – VERO

---

50) La crittografia permette di proteggere le quattro proprietà di sicurezza dell'informazione: riservatezza, integrità, autenticità e disponibilità – FALSO *(freq. 2)*

Non permette di protteggere la disponibilità delle informazioni.

---

51) Nel modello Infrastrutturale della certificazione delle chiavi pubbliche l'autenticità della chiave pubblica è data da un soggetto terzo fidato che emette la certificazione – VERO *(FREQ. 2)*

N.B.: La domanda, con questo, intende la certification authority

---

52) Nel modello web of trust della certificazione delle chiavi pubbliche l'autenticità della chiave pubblica è attestata dagli altri utenti – VERO *(freq. 2)*

N.B.: intende pgp.

---

53) Uno dei presupposti per la robustezza degli algoritmi a chiave asimmetrica è che non esistono modi efficenti di fattorizzare il modulo – VERO

---

54) Secure Boot è il nome specifico dato all'implementazione di trusted boot basata su UEFI – VERO

---

55) I sistemi SIEM raccolgono dati che devono essere nativamente omogenei per poter essere confrontati e aggregati – FALSO *(freq. 2)*

I dati non sono omogenei, ma derivano da più fonti. Il SIEM poi rileva le correlazioni, e collega gli attributi comuni.

---

56) Il kernel di Linux permette di porre sotto monitoraggio l'invocazione di ogni system call – VERO *(freq. 2)*

n.b.: lo fa con auditd.

---

57) Il controllo dell'integrità dei file è uno dei metodi usati dagli HIDS – VERO *(FREQ. 2)*

---

58) X.509 è la versione di SSL più utilizzata - FALSO

X509 non è una versione di SSL, bensì una PKI (e quindi anche un tipo di certificato).

---

59) 802.1x è uno standard di autenticazione utilizzato nelle connessioni fisiche – VERO

---

60) Le botnet sono reti di computer infetti chiamati zombie – VERO *(FREQ. 2)*

---

61) È possibile esfiltrare dati attraverso richieste DNS – VERO

---

62) Nelle time based sql-injection è importante il tempo di computazione della query sql – VERO

---

63) Il registro EIP in x86 salva il valore dell'indirizzo di ritorno da una funzione – FALSO

EIP contiene il puntatore all'ultima istruzione, EDI invece contiene l'indirizzo di ritorno.

---

64) Con una Local File Inclusion possiamo recuperare file interni al web server – VERO *(FREQ. 2)*

---

65) Data chiave pubblica (e, n) e chiave privata (d, n) la cifratura consiste nel calcolare:
c = m^e mod n – VERO

---

66) Il salt è una password aggiuntiva di secondo livello – FALSO

Il salt è variazione random inserita alla scelta della password.

---

67) La fiducia nell'autenticità di una Root Certification Authority è perfettamente verificabile dal corrispondente certificato – FALSO

Non abbiamo modo di dimostrare che la Root Certification Authority sia effettivamente non malevola, ma ci fidiamo ciecamente ad essa.

---

68) Measured Boot si riferisce a un processo generale, che tipicamente usa un TPM come hardware root of trust – VERO

---

69) L'IP spoofing consiste nell'assumere un indirizzo IP diverso da quello regolarmente assegnato al proprio sistema – VERO

---

70) La collocazione di sistemi in cloud ha unicamente effetti positivi sulla sicurezza – FALSO

Uno degli effettivi negativi, per esempio, è il possibile vendor lock-in.

---

71) Nelle SQL Injection di tipo union select, il numero di colonne da usare per la query è un dato fondamentale per la riuscita dell'attacco – VERO *(freq. 2)*

---

72) I log sono utili solo a fini forensi (cioè per comprendere un attacco dopo che si è compiuto) – FALSO

Possiamo anche esaminare i log in tempo reale con un HIDS, per esempio.

---

73) Tra i fattori di autenticazione c'è qualcosa che si possiede fisicamente, come un Pin o una Password – FALSO *(freq. 2)*

Un pin/password sono classificati come “qualcosa che si sa”, e non qualcosa che si ha fisicamente.

---

74) 2FA e 2 step authentication sono esattamente la stessa cosa – FALSO *(freq. 2)*

Nel 2-step-authentication, il livello aggiuntivo non viene riconosciuto come un livello distinto.
Nel 2FA, invece, si usano due fattori “diversi”, per esempio qualcosa che si ha + qualcosa che si sa.

---

75) L'ARP poisoning consiste nel convincere un host che l'IP di una vittima è associato al MAC dell'attaccante - VERO

---

76) Nel modello RBAC (Role-based access control) i permessi sono assegnati ai ruoli - VERO

---

77) I cifrari classici possono essere impiegati per proteggere riservatezza e autenticità – FALSO

I cifrari classici non permettono di proteggere l’autenticità, siccome non fanno uso di chiave asimmetrica.

---

78) Gli algoritmi di cifratura a blocchi sono così definiti perchè si arrestano non appena la cifrazione è considerata sicura – FALSO

Gli algoritmi di cifratura a blocchi sono degli algoritmi che cifrano “a blocchi” (ovvero dividendo in sequenze di dimensione fissa) il testo.

---

79) DH e RSA hanno scopi differenti: quello di RSA é di scambiarsi la chiave simmetrica di cifratura – FALSO

Un po’ ambigua, ma si intende il fatto che lo scopo principale di RSA sia quello, quando invece tutto ciò che fa è creare un canale sicuro per la comunicazione della chiave simmetrica. In questo caso, DH si occupa dello scambio.

---

80) Esistono tre tipi fondamentali di firewall Packet filter, Application-level gateway, Circuit-level gateway – VERO

---

81) Un EDR può essere definito come una variante evoluta di Network-based IDS – FALSO

È un tipo di HIDS.

---

82) Il Command and Control è il computer incaricato di gestire le comunicazioni con gli elementi di una botnet – VERO

---

83) Appropriarsi dell'indirizzo di un host può permettere di attaccarlo di riflesso - VERO

---

84) Code Injection si verifica quando dell'input non sanitizzato viene interpretato come codice – VERO

---

85) Se un sito è protetto da TLS non è possibile eseguire una SQL Injection – FALSO

Ovviamente no, TLS ci protegge principalmente dall’intercettazione dei dati.

Fine domande...